IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA
CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. LI SHAOMING, MO HAILONG, a/k/a Robert Mo, WANG LEI, WANG HONGWEI, YE JIAN, LIN YONG and MO YUN, Defendants.	Criminal No. 4:13-cr-147 **BRIEF IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE OBTAINED UNDER FISA AND THE FRUITS OF SUCH EVIDENCE**

This case involves a breathtaking and unprecedented expansion of the government's use of the Foreign Intelligence Surveillance Act ("FISA"). As the court charged with overseeing the statute has recognized, "FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security." *In re Sealed Case*, 310 F.3d 717, 739 (FISA Ct. R. 2002). In keeping with its narrow purpose, FISA surveillance must target a "foreign power" or an "agent of a foreign power;" a "significant purpose" of the surveillance must be to obtain "foreign intelligence information;" and the surveillance may only be used when the information at issue cannot reasonably be obtained by normal investigative techniques.

The FISA surveillance at issue here ignored these strict limitations. For the first time in the statute's history (as far as our research reveals), the government used FISA to investigate a trade secret dispute between two privately-owned companies.[1] There was no "foreign power" or "agent of a foreign power;" the information sought was not "foreign intelligence information;"

[1] We use the phrase "privately-owned company" in this brief to refer to companies whose stock is owned by non-state persons or entities. The phrase includes both companies whose stock trades on a public exchange and companies whose stock is not publicly traded.

and that information could have been obtained through normal investigative techniques. Because the surveillance exceeded what FISA allows and violated Defendant Mo's Fourth Amendment rights, the Court should suppress the FISA surveillance and its fruits.

INTRODUCTION

Mo Hailong ("Mr. Mo") has been charged with conspiracy to steal trade secrets in the form of corn germplasm. Doc. 57. Mr. Mo, a legal permanent resident of the United States who formerly lived in Boca Raton, Florida with his wife and two children, serves as Director of International Business of Beijing Daibeinong Technology Group ("DBN"). The indictment alleges that Mr. Mo purchased and collected corn seeds in Iowa and elsewhere, and then mailed corn seeds (allegedly those he collected or purchased) back home to Florida and to an undisclosed address in China. Mr. Mo allegedly planted another group of seeds on farmland that he purchased.

That is the totality of the conduct alleged: corn seed purchase, corn seed collection, and some planting, storage, and transportation of seeds – hardly a "particularly serious . . . foreign threat[] to national security." Yet, apparently for the first time in the history of FISA, the statute has been used to conduct surveillance in connection with an alleged effort by one privately-owned company to steal non-defense-related trade secrets from another privately-owned company.

For the reasons that follow, the FISA evidence must be suppressed. Part I outlines the purpose and structure of FISA. Part II maintains that the applications to the Foreign Intelligence Surveillance Court ("FISC") did not establish probable cause to believe that Mr. Mo (or any other possible target of the FISA surveillance) was a "foreign power" or an "agent of a foreign power." As the Declaration of Dr. Tong Yao (attached as Exhibit 1) demonstrates, DBN is a

privately-owned company; it is neither owned nor controlled by the Chinese government. It is not a "foreign power," and its employees (including Mr. Mo) are not "agents of a foreign power." Part III contends that the government's certifications to the FISC concerning "foreign intelligence information" were clearly erroneous, because the information sought was not "necessary to . . . the ability of the United States to protect against . . . clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power." 50 U.S.C. § 1801(e)(1)(C). Part IV maintains that the government's "necessity" certifications were clearly erroneous, because normal investigative techniques could have obtained the information at issue. Part V asks the Court to determine whether the government adopted and implemented proper minimization procedures. Finally, Part VI challenges the applications to the FISC under *Franks v. Delaware*, 438 U.S. 154 (1978), and its progeny and requests a *Franks* hearing.

We must necessarily make these arguments in a vacuum, because we have not received access to the underlying FISA applications, orders, and related materials. We do not even know the identity of the target of the FISA surveillance, or what evidence the government obtained through FISA; it has refused to provide even that limited information. Docket No. 177. We have moved to require the government to identify the evidence it obtained through FISA and other surveillance techniques, Docket No. 153,[2] and we are filing today a motion for disclosure of the underlying FISA applications, orders, and related materials. If the Court orders disclosure, we request an opportunity to supplement this motion after reviewing the FISA materials.

[2] Chief Magistrate Judge Bremer denied Mr. Mo's motion for notice of the evidence obtained through FISA and other investigative techniques. Docket No. 214. Mr. Mo intends to appeal that order.

ARGUMENT

I. THE PURPOSE AND STRUCTURE OF FISA.

Congress enacted FISA in response to *United States v. United States District Court for the Eastern District of Michigan (Keith)*, 407 U.S. 297 (1972).[3] In *Keith*, the Supreme Court held that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. The Court noted the intrusiveness of electronic surveillance and cautioned that "[t]he historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Id.* at 317. The Court invited Congress to legislate standards for intelligence-related surveillance that "differ from those already prescribed for specified crimes in Title III." *Id.* at 322.

FISA was also a response to the Report of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee Report),[4] which found that the executive had engaged in warrantless wiretapping of numerous citizens–including journalists, political activists, and members of Congress–who posed no threat to the nation's security and who were not suspected of any criminal offense. Thus, FISA "was enacted to create a framework whereby the Executive could conduct electronic surveillance for foreign

---

[3] *See, e.g.,* S. Rep. 604(I), 95th Cong., 1st Sess. 13-14, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3914-16; S. Rep. 701, 95th Cong., 1st Sess. 9, 15-16, *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977, 3984-85.

[4] *See* S. Rep. 604(I), 95th Cong., 1st Sess. 7 (Senate Judiciary Committee Report: "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused," citing Church Committee report), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908; S. Rep. 701, 95th Cong., 1st Sess. 9 (Senate Intelligence Committee Report with similar remark), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977.

intelligence purposes without violating the rights of citizens."[5] The Act "was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties."[6]

FISA seeks to accomplish this "sound balance" through several key provisions. *First*, FISA creates the FISC, to which the government must apply for an order authorizing electronic surveillance, 50 U.S.C. §§ 1803, 1804, or a physical search, *id.* § 1823.[7] As the United States Court of Appeals for the Fourth Circuit has observed, "[W]ith certain exceptions . . . a FISA judge must approve in advance all electronic surveillance of a foreign power or its agents."[8]

Second, the statute requires that the government's application to the FISC include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[9] The application must also contain certain "certifications" by an appropriate executive branch official. Among other things, the official must certify that he or she "deems the information sought to be foreign intelligence information" and that "a significant purpose of the surveillance is to obtain foreign intelligence information."[10] In addition, the certification must "designate[] the type of foreign intelligence information being sought according to the categories described in" 50 U.S.C. § 1801(e) and include "a statement of the basis for the certification that . . . the information

---

[5] *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (en banc), *vacated on other grounds*, 543 U.S. 1097 (2005), *reinstated in relevant part*, 405 F.3d 1034 (4th Cir. 2005) (en banc).

[6] *In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (quotation omitted).

[7] The FISA provisions governing physical searches generally parallel the provisions governing electronic surveillance. Although our argument applies to both sets of provisions, for the sake of simplicity we refer solely to the electronic surveillance provisions.

[8] *Hammoud*, 381 F.3d at 332; *see, e.g., United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988); *United States v. Cavanagh*, 807 F.2d 787, 788 (9th Cir. 1987).

[9] 50 U.S.C. § 1804(a)(3)(A); *United States v. Posey*, 864 F.2d 1487, 1490 (9th Cir. 1989).

[10] 50 U.S.C. § 1804(a)(6)(A), (B).

sought is the type of foreign intelligence information designated."[11]

Third, the statute specifies findings that the FISC must make before it can approve electronic surveillance.[12] The court must find that the procedural requirements of FISA have been satisfied,[13] including the minimization requirements, and it must find (among other things) "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[14] When the target of the surveillance is a "United States person"–including a lawful permanent resident alien such as Mo[15]–the FISC must also determine that the government's certifications are not "clearly erroneous."[16]

Fourth, FISA requires notice to the target of the surveillance when the government "intends to enter into evidence or otherwise use or disclose" the fruits of FISA surveillance or a FISA search against an "aggrieved person" in any proceeding in a federal court.[17] FISA defines "aggrieved person" as "a person who is the target of electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[18] Under these definitions, Mr. Mo is an "aggrieved person" for the electronic surveillance that targeted him or intercepted his communications. *See, e.g., United States v. Cavanagh*, 807 F.2d 787, 789 (9th Cir. 1987). The statute authorizes any "aggrieved person" to move to suppress "evidence

---

[11] *Id.* § 1804(a)(6)(D), (E)(i).

[12] *Id.* § 1805.

[13] *E.g., id.* §§ 1805(a)(1), (3), (4).

[14] *Id.* § 1805(a)(2)(A); *see, e.g., Dumeisi*, 424 F.3d at 579; *Hammoud*, 381 F.3d at 332-33 (discussing probable cause requirement).

[15] 50 U.S.C. § 1801(i) (defining "United States person" to include "an alien lawfully admitted for permanent residence").

[16] *Id.* § 1805(a)(4).

[17] *Id.* § 1806(c).

[18] *Id.* § 1801(k).

obtained or derived from" electronic surveillance if "the information was unlawfully acquired" or "the surveillance was not made in conformity with an order of authorization or approval."[19]

We discuss the FISA procedures in more detail below.

II. THE APPLICATIONS DO NOT ESTABLISH PROBABLE CAUSE TO BELIEVE THAT THE TARGET OF THE SURVEILLANCE WAS A FOREIGN POWER OR AN AGENT OF A FOREIGN POWER.

Before issuing a FISA surveillance order, the FISC must find probable cause to believe that the target "is a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2)(A). "In determining whether probable cause exists under this section, the court must consider the same requisite elements which govern such determinations in the traditional criminal context." S. Rep. 701, 95th Cong., 1st Sess. 53, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4022.[20] Without disclosure of the FISA materials, we do not know whether the target of the FISA surveillance was Mo or some other person or entity. Nonetheless, we are confident that, if the applications to the FISC were accurate and complete, they did not establish probable cause to believe that the target was either a "foreign power" or an "agent of a foreign power."[21]

---

[19] *Id.* § 1806(e). Section 1806 includes procedures for disclosure of the underlying applications, orders, and other materials. We discuss those procedures in the accompanying motion for disclosure of FISA materials.

[20] In assessing the applications' probable cause showing, the Court should examine raw intelligence with a critical eye. *See Obaydullah v. Obama*, 688 F.3d 784, 792 (D.C. Cir. 2012) (on review of a Guantanamo detainee's habeas petition, noting criteria for deciding whether evidence is sufficient to characterize the petitioner as a member of al Qaeda)

[21] The Court should review the FISC's probable cause finding de novo. *See, e.g., United States v. Dumeisi*, 424 F.3d 526, 578 (7th Cir. 2005); *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *United States v. Huang*, 15 F. Supp. 3d 1131, 1138 (D.N.M. 2014); *United States v. Warsame*, 547 F. Supp. 2d 982, 990 (D. Minn. 2008); *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006).

A. Foreign Power.

FISA defines "foreign power" to include, among other entities, "a foreign government or any component thereof whether or not recognized by the United States" and "an entity that is directed and controlled by a foreign government."[22] The PRC government is a "foreign power," but it has no involvement in this case. That is undoubtedly why the prosecution charged the case as a conspiracy to steal trade secrets in violation of 18 U.S.C. § 1832, rather than a conspiracy to commit economic espionage on behalf of a foreign government in violation of 18 U.S.C. § 1831. If the prosecution had any evidence that the PRC government was involved in the alleged germplasm theft, it would have charged the case under § 1831, which carries more severe penalties. *Compare, e.g., United States v. Chung*, 659 F.3d 815 (9th Cir. 2011) (charging violation of 18 U.S.C. § 1831 where defendant was alleged to have stolen trade secrets for the benefit of the PRC).

DBN is the only other potential "foreign power." But there is no reliable evidence – much less probable cause to believe – that DBN is "directed and controlled" by the PRC government. *See, e.g.*, S. Rep. 701, *supra*, at 18, 1978 U.S.C.C.A.N. at 3987 ("[I]t is important to emphasize that the judge must find probable cause that the entity is both 'directed' and 'controlled' by a foreign government or governments."). To the contrary, as Dr. Yao's declaration establishes, DBN has been privately owned and controlled at all relevant times. The PRC owned no stock in the company in 2011 and 2012, and it owned slightly over 1% in 2013 and 2014 through the National Social Insurance Fund, which is managed by professional investment managers. Yao Dec. ¶ 16. That negligible interest plainly does not amount to PRC direction or control. As Dr. Yao explains:

[22] 50 U.S.C. § 1801(a)(1), (6).

> In sum, based on my extensive research into the ownership of DBN, and my knowledge of Chinese financial markets, I concluded that at no time from 2011 through 2014 has DBN been controlled by the Chinese government, any subdivision thereof, or any Chinese government-controlled entity. Nor has the Chinese government owned more than a *de minimus* stake in DBN during that period. DBN has been and remains privately owned and controlled.

Yao Dec. ¶ 22.

B. Agent of a Foreign Power.

An "agent of a foreign power," as applied to a "United States person" such as Mo, means (as potentially relevant here) "any person who knowingly engages in *clandestine intelligence gathering activities for or on behalf of a foreign power*, which activities involve or may involve a violation of the criminal statutes of the United States," and "any person who knowingly aids or abets [or conspires with] any person in the conduct of activities" described above.[23]

For two reasons, the applications – to the extent they are accurate and do not omit material facts – do not establish probable cause to believe that Mo or any other potential target of the FISA surveillance was an "agent of a foreign power." First, there is no evidence that Mo or any other potential target acted "for or on behalf of a foreign power." As the Senate Judiciary Committee explained, "Under this standard the person to be surveilled must be shown to have a knowing and substantial connection with the foreign power for whom he is working. There must be a principal-agent relationship under which the alleged agent has undertaken to provide services for his foreign principal." S. Rep. 95-604(I), 95th Cong., 1st Sess. 22, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3923. Neither Mo nor any other potential surveillance target had a "knowing and substantial connection" or a "principal-agent relationship" with the PRC. And although Mo did have both a "knowing and substantial connection" and a "principal-agent relationship" with DBN, that company is not a "foreign power," as explained above.

[23] 50 U.S.C. § 1801(b)(2)(A), (E) (ellipses omitted; emphasis added).

Second, there is no evidence that Mo or any other potential target engaged in "clandestine intelligence gathering activities." According to the Senate Intelligence Committee, "most of the persons under surveillance under this subparagraph will be violating the criminal espionage laws which appear in title 18, United States Code, sections 792-799, 951; title 42, United States Code, sections 2272-2278b; and title 50, United States Code, section 855." S. Rep. 701, *supra*, at 21, *reprinted in* 1978 U.S.C.C.A.N. at 3990.[24] The Intelligence Committee Report adds:

> Apart from the types of activities specifically proscribed by the espionage laws, this subparagraph is also intended to permit the surveillance of foreign intelligence agents who are collecting industrial or technological information *which, if disclosed to a hostile foreign power, might present a threat to the security of the nation.* In such a case, the Government would have to establish that the agent was collecting or transmitting such information in a manner which might involve a violation of some other Federal statute, such as title 18, United States Code, section 2514, which proscribes the interstate transportation of stolen property. . . .
>
> *Otherwise, clandestine collection of information regarding the unclassified business plans or trade secrets of an American company which merely might provide a competitive advantage to private foreign firms, for example, in bidding on a contract with a third country, would not be "clandestine intelligence gathering activity."*

Id. at 22 (emphasis added), *reprinted in* 1978 U.S.C.C.A.N. at 3991.

This legislative history confirms that neither Mo nor any other surveillance target was engaged in "clandestine intelligence gathering activity." The corn germplasm that Mo allegedly conspired to steal obviously does not "present a threat to the security of the nation." His alleged "clandestine collection of information" concerned the "unclassified . . . trade secrets of an American company which merely might provide a competitive advantage to private foreign

[24] Neither Mo nor anyone else has been charged under the "criminal espionage laws." Of particular significance, neither Mo nor anyone else has been charged under the Foreign Agent Registration Act, 18 U.S.C. § 951, with operating as an unregistered foreign agent. *Compare, e.g., United States v. Chung*, 659 F.3d 815 (9th Cir. 2011) (charging violation of FARA, among other offenses, where defendant was alleged to have stolen trade secrets for the benefit of the PRC).

firms" – precisely the conduct that, according to the Senate Intelligence Committee, "would not be 'clandestine intelligence gathering activity.'"

For these reasons, the FISA applications – to the extent they were accurate and complete – could not have established probable cause to believe that Mo or any other potential target of the surveillance was an "agent of a foreign power."

III. THE GOVERNMENT'S CERTIFICATIONS CONCERNING "FOREIGN INTELLIGENCE INFORMATION" ARE CLEARLY ERRONEOUS.

The government's applications to the FISC presumably contained "certifications" by an appropriate executive branch official that he or she "deems the information sought to be foreign intelligence information" and that "a significant purpose of the surveillance is to obtain foreign intelligence information."[25] In addition, the certifications "designate[d] the type of foreign intelligence information being sought according to the categories described in" 50 U.S.C. § 1801(e) and included "a statement of the basis for the certification that . . . the information sought is the type of foreign intelligence information designated."[26] Because Mo is a "United States person," the FISC and this Court review the certifications for clear error. 50 U.S.C. § 1805(a)(4); *see United States v. Warsame*, 547 F. Supp. 2d 982, 990 (D. Minn. 2008).

As the certification requirements indicate, obtaining "foreign intelligence information" is the central goal of FISA surveillance. The phrase includes, as potentially relevant here, "information that . . . is necessary to . . . the ability of the United States to protect against . . . clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power." 50 U.S.C. § 1801(e)(1)(C). According to the Senate Intelligence

[25] 50 U.S.C. § 1804(a)(6)(A), (B). Here and elsewhere, we assume that the applications (which we have not seen) contained the certifications required by statute. If any certification was omitted, of course, the application did not comply with FISA, and any resulting evidence must be suppressed. *Id.* § 1806(e).

[26] *Id.* § 1804(a)(6)(D), (E)(i).

Committee, the term "necessary" in § 1801(e)(1) "require[s] more than a showing that the information would be useful or convenient. The committee intends to require that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance." S. Rep. 701, *supra*, at 31, *reprinted in* 1978 U.S.C.C.A.N. at 4000.

Under these standards, the "foreign intelligence information" certifications in the FISA applications are clearly erroneous. The government has no "significant need" for information about the alleged theft of corn germplasm to protect the United States against "clandestine intelligence activities" by "an agent of a foreign power." No "clandestine intelligence activities" are involved here, because disclosure of the germplasm to a "hostile foreign power" could not possibly "present a threat to the security of the nation." *Id.* at 22 (emphasis added), *reprinted in* 1978 U.S.C.C.A.N. at 3991. And, for the reasons outlined in Part II, neither Mo nor any other alleged conspirator was "an intelligence service or network of a foreign power" or "an agent of a foreign power."

IV. THE GOVERNMENT'S "NECESSITY" CERTIFICATIONS WERE CLEARLY ERRONEOUS.

The FISA applications certify that the purported foreign intelligence information "cannot reasonably be obtained by normal investigative techniques."[27] In addition, the certifications include "a statement of the basis for the certification that . . . such [foreign intelligence] information cannot reasonably be obtained by normal investigative techniques."[28] The Senate Intelligence Committee identified this "necessity" certification as an important safeguard for privacy. *Id.* at 11, *reprinted at* 1978 U.S.C.C.A.N. at 3980.

---

[27] *Id.* § 1804(a)(6)(C).

[28] *Id.* § 1804(a)(6)(E)(ii).

Because the government has refused to say what evidence it obtained through FISA, *e.g.*, Doc. 177, we cannot address these "necessity" certifications with specificity. At least some of the potential FISA evidence – for example, recordings obtained from listening devices placed in automobiles in the United States – plainly could have been obtained through Title III surveillance or other "normal" techniques, such as the use of confidential informants.

In addition, the government used a host of other "normal" techniques, including search warrants, national security letters, requests for information under 18 U.S.C. § 2703(d), and pole cameras. For example, the government obtained a warrant to search Mo's home and office and seized computers and hard drives; financial, scientific, and general company papers; seed samples; and photographs. During a warrant search of a storage locker in Adel, Iowa, the government obtained 26 bags of seed; 12 empty seed bags; a bag full of cob corn; net bags; and photographs. The government obtained additional seeds during a warrant search of five boxes of corn, shipped via FedEx. The government also obtained warrants to search bags of seeds along with other material seized during the Customs and Border Patrol searches of Ye Jian, Li Shaoming, and Wang Hongwei.

A warrant for emails from the Yahoo email accounts of both Mo and Lang Deng allowed collection of the contents of all emails from January 2010 through March 29, 2012, along with all records and other information related to the account. The government also obtained a warrant to search Mo Yun's iPhone, as well as a warrant for location data from Mo's T-Mobile cell phone during 2012. Through subpoenas, the government obtained Mo's bank records, among other material. And through a warrant to Apple, the government obtained more than 2,000 documents from Mo's iCloud account, including contents of stored emails; contacts; calendar data; pictures; files; and account records.

The government has failed to produce all tracking warrants and information obtained by the warrants, but related documents – a motion to seal and delay notification of a tracking warrant, for example – indicate the government also secured warrants for the installation of GPS tracking devices on vehicles Mo and certain of his co-defendants drove. The government's incomplete production shows these warrants yielded voluminous location data about several vehicles in 2012.

The government obtained court orders under 18 U.S.C. § 2703 for stored electronic records from Dong Zhanshan's Google accounts; DBN's DropBox account; Mo's Google records; and the Google, Hotmail, and MSN records of Zhao Lijuan. In addition, the government obtained pen registers on two phones, including Mo's cell phone, during 2012.

As set forth in the chart attached as Exhibit 2, these and other "normal investigative techniques" produced an enormous amount of information. If the government had continued their use, the techniques may well have yielded the information the government obtained through FISA (whatever that information is). We will seek leave to supplement our argument on the "necessity" certifications if the Court grants Mo's motion for notice of the evidence obtained through FISA and other investigative techniques (Doc. 153) or the motion for disclosure of FISA materials filed with this motion.

V. THE GOVERNMENT'S MINIMIZATION WAS INADEQUATE.

The government's applications to the FISC provided a "statement of the proposed minimization procedures."[29] FISA requires minimization procedures that "are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information

[29] *Id.* § 1804(a)(4).

concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[30] The minimization procedures must also "require that nonpublicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance."[31] Congress intended these procedures to serve as "vital safeguards." S. Rep. 701, *supra*, at 39, *reprinted in* 1978 U.S.C.C.A.N. at 4008. As one court explained soon after FISA was enacted, the statutory scheme "centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance." *United States v. Belfield*, 692 F.2d 141, 148 n.34 (D.C. Cir. 1982) (footnote omitted) (quoting Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing their Job*, 12 Rutgers L.J. 405, 408 (1981)).[32]

---

[30] *Id.* § 1801(h)(1). The statute adds that, notwithstanding these provisions, minimization procedures may "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." *Id.* § 1801(h)(3); *In re Sealed Case*, 310 F.3d 717, 731 (Foreign Intelligence Surveillance Court of Review 2002) (discussing FISA minimization procedures).

[31] 50 U.S.C. § 1801(h)(2).

[32] Despite the statute's emphasis on minimization as a privacy safeguard, courts have held that the FISA minimization provisions permit the government to record automatically all intercepted communications and to eliminate the non-foreign intelligence information later, when the surveillance tapes are logged and indexed. *See, e.g., Hammoud*, 381 F.3d at 334; *In re Sealed Case*, 310 F.3d at 740-41; *United States v. Sattar*, 2003 U.S. Dist. LEXIS 16164, at *28-*35 (S.D.N.Y. Sept. 15, 2003); *In re Kevork*, 634 F. Supp. 1002, 1016-17 (C.D. Cal. 1985), *aff'd on other grounds*, 788 F.2d 566 (9th Cir. 1986). As a result of this around-the-clock surveillance, FISA wiretaps routinely intercept attorney-client, husband-wife, and other privileged communications.

The government appears not to have complied with FISA's "vital" minimization procedures in this case. For example, transcripts of the recordings obtained through the car bugs demonstrate that much of the captured material is entirely irrelevant to the investigation; the recordings were not minimized either at the time of the recording or even upon later review. In light of this possible failure to comply with the minimization requirements, the Court should subject the government's minimization procedures and the effectiveness of those procedures to "close judicial review." S. Rep. 701, *supra*, at 50, *reprinted in* 1978 U.S.C.C.A.N. at 4019.

VI. A *FRANKS* HEARING IS WARRANTED BECAUSE THE FISA APPLICATIONS MAY CONTAIN INTENTIONAL OR RECKLESS MATERIAL FALSEHOODS AND OMISSIONS.

In each FISA application, the government provided information to the FISC that convinced it to find probable cause that Mo (or another target of the surveillance that intercepted Mo's communications) was a "foreign power" or an "agent of a foreign power." Each application included a "statement of the basis for the certification that . . . the information sought is the type of foreign intelligence information designated."[33] And each application included "a statement of the basis for the certification that . . . such [foreign intelligence] information cannot reasonably be obtained by normal investigative techniques."[34] For the reasons outlined above, the government could not have obtained the FISC's approval for the surveillance if the information it provided in the applications on these issues had been accurate and complete. Accordingly, Mo requests an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154 (1978).

Under *Franks*, a court must hold an evidentiary hearing on the veracity of a warrant if the defendant makes a "substantial preliminary showing" that the underlying affidavit contains intentional or reckless false statements or omissions and that the false or omitted information was

[33] 50 U.S.C. § 1804(a)(6)(D), (E)(i).

[34] *Id.* § 1804(a)(6)(E)(ii).

material to the probable cause finding. *See id.* at 155-56; *United States v. Jacobs*, 986 F.2d 1231, 1233-34 (8th Cir. 1993) (suppression warranted based on intentional or reckless material omissions). Courts have repeatedly recognized that *Franks* applies to FISA applications. *See United States v. Daoud*, 755 F.3d 479, 489 (7th Cir. 2014) (Rovner, J., concurring) (collecting cases), *cert. denied*, 2015 U.S. LEXIS 1309 (U.S. Feb. 23, 2015).

Although *Franks* applies in the FISA context, to date no federal court has held a *Franks* hearing to review a FISA order. This is because the secret, *ex parte* nature of the proceedings makes it virtually impossible for the defendant to make the "substantial preliminary showing" that *Franks* requires. As one court put it, "The quest to satisfy the *Franks* requirements [in the FISA context] might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility." *United States v. Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *17 (N.D. Ill. Nov. 10, 2010). Judge Rovner made a similar point in her *Daoud* concurrence: "As a practical matter, the secrecy shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks* absent a patent inconsistency in the FISA application itself or a sua sponte disclosure by the government that the FISA application contained a material misstatement or omission." *Daoud*, 755 F.3d at 486 (Rovner, J., concurring).

Despite the extraordinary difficulty of making a *Franks* showing in the FISA context, Mo has attempted to do so here. We have reason to believe that the government argued to the FISC that DBN is "an entity that is directed and controlled by a foreign government" – the PRC – and thus is a "foreign power."[35] As Dr. Yao's declaration demonstrates, that representation

[35] 50 U.S.C. § 1801(a)(1), (6).

(assuming it was made) was materially false. DBN was privately owned and controlled throughout the relevant period. Yao Dec. ¶¶ 18-22. For similar reasons, the applications to the FISC likely contained material omissions on the "foreign power" requirement. For example, the applications likely omitted the information on which Dr. Yao relies, all of which "was and is publicly available." Yao Dec. ¶ 23. We thus ask the Court to examine the applications to the FISC with great care to determine whether, in light of the Yao declaration, Mo has made a "substantial preliminary showing" that the applications contain intentional or reckless material misstatements or omissions on the "foreign power"/"agent of a foreign power" issue.[36]

Similarly, with respect to each application the Court should examine with care the "statement of the basis for the certification that . . . the information sought is the type of foreign intelligence information designated" and the "statement of the basis for the certification that . . . such [foreign intelligence] information cannot reasonably be obtained by normal investigative techniques." For the reasons outlined above, the government could only have convinced the FISC that the foreign intelligence information and necessity certifications were not clearly erroneous by either recklessly misstating material facts or recklessly omitting material facts.

Unless the Court can determine from examining the FISA applications ex parte in light of the Yao declaration and the other information Mo has submitted that a *Franks* hearing is warranted, it should order disclosure of the underlying FISA applications, orders, and related materials to defense counsel under "appropriate security procedures and protective orders." 50 U.S.C. § 1806(f). As the accompanying FISA disclosure motion shows, disclosure would

[36] Mo will file with his other suppression motions an omnibus pleading outlining the falsehoods and omissions in search warrant affidavits and other formal submissions the government made during the investigation of this matter. We ask the Court to examine the FISA applications carefully to determine whether any of those falsehoods and omissions appear in the FISA applications.

substantially promote an accurate determination of Mo's *Franks* claim. Following disclosure, the Court should permit defense counsel to supplement the *Franks* argument outlined above.

If the Court declines to order the disclosure we have requested, it should pursue an alternative form of investigation. As Judge Rovner put it, "Courts must do what they can to compensate for a defendant's ignorance as to what the FISA application contains. Otherwise, *Franks* will persist in name only in the FISA setting." *Daoud*, 755 F.3d at 495 (Rovner, J., concurring). We propose the following as a poor, but necessary, substitute for disclosure: The Court should first review the FISA applications and accompanying materials *in camera*, evaluating the type of evidence presented and considering what gaps it might leave. The Court should then identify in unclassified form (with the assistance, if necessary, of a Court Security Officer) any arguable misstatements or omissions it has found and request further information on those issues from both parties. To the extent the government is permitted to submit information to the Court *ex parte*, the defense should be given the same opportunity. *Cf. United States v. Clegg*, 740 F.2d 16, 17 (9th Cir. 1984) (district court accepted *ex parte* submissions from both sides on discovery issues); *United States v. Libby*, 429 F. Supp. 2d 18, 26 (permitting defense to submit *ex parte* affidavit from counsel to assist court in considering whether government's proposed redactions and substitutions are appropriate), *amended on other grounds*, 429 F. Supp. 2d 46 (D.D.C. 2006); *United States v. Poindexter*, 727 F. Supp. 1470, 1479 & n.16 (D.D.C. 1989) (permitting defense to explain *ex parte* the relevance of certain documents); *United States v. North*, 698 F. Supp. 322, 324 (D.D.C. 1988) (with agreement of prosecution, court heard a four hour ex parte defense presentation concerning the defendant's need for classified discovery he had requested).

This procedure will not compensate for a lack of disclosure of the FISA applications, orders, and other materials. But it would at least give the defense *some* chance of making the "substantial preliminary showing" that *Franks* requires for an evidentiary hearing.

CONCLUSION

For the foregoing reasons, the Court should enter an Order suppressing all evidence obtained under FISA and the fruits of such evidence.

WEINHARDT & LOGAN, P.C.

By _____
Mark E. Weinhardt AT0008280
Holly M. Logan AT0004710

2600 Grand Avenue, Suite 450
Des Moines, IA 50312
Telephone: (515) 244-3100
E-mail: mweinhardt@weinhardtlogan.com
hlogan@weinhardtlogan.com

LAW OFFICE OF MARK BECK

By _____
Mark Beck (Admitted pro hac vice)

350 West Colorado Blvd, Suite 200
Pasadena, CA 91105
Telephone: (626) 234-5334
Email: mbeck@markbecklaw.com
ATTORNEYS FOR MO HAILONG, ALSO KNOWN AS ROBERT MO

PROOF OF SERVICE

The undersigned certifies that the foregoing instrument was served upon the parties to this action by serving a copy upon each of the attorneys listed below on March 13, 2015, by

- ☐ U.S. Mail
- ☐ FAX
- ☐ Hand Delivered
- ☐ Electronic Mail
- ☐ FedEx/ Overnight Carrier
- ☒ CM / ECF

Jason T. Griess
U.S. Attorney's Office
jason.griess2@usdoj.gov

Marc Krickbaum
marc.krickbaum@usdoj.gov

Leon F. Spies
Mellon & Spies
Spieslegal@aol.com

Terry W. Bird
Bird Marella
TWB@birdmarella.com

ATTORNEYS FOR MO YUN

Signature: MyBaldus